What is claimed is:

1. A cryptocommunication system including a transmission apparatus and a reception apparatus,

the transmission apparatus encrypting plaintext to generate ciphertext, performing a one-way operation on the plaintext to generate a first value, and transmitting the ciphertext and the first value to the reception apparatus,

the reception apparatus receiving the ciphertext and the first value, decrypting the ciphertext to generate decrypted text, performing the one-way operation on the decrypted text to generate a second value, and judging that the decrypted text matches the plaintext when the second value and the first value match,

the transmission apparatus comprising:

first generating means for generating first additional information;

first operation means for performing an invertible operation on the plaintext and the first additional information to generate connected information;

encrypting means for encrypting the connected information according to an encryption algorithm to generate the ciphertext; and

transmitting means for transmitting the ciphertext,

the reception apparatus comprising:

receiving means for receiving the ciphertext;

second generating means for generating second additional information which is identical to the first additional information;

decrypting means for decrypting the ciphertext according to a decryption algorithm which is an inverse-conversion of the encryption algorithm so as to generate decrypted connected information; and

second operation means for performing an inverse operation of the invertible operation on the decrypted connected information and the second additional information so as to generate the decrypted text.

2. The cryptocommunication system of Claim 1,

wherein the second generating means synchronizes with the first generation means so as to generate the second additional information which is identical to the first additional information.

3. The cryptocommunication system of Claim 1,

wherein the first generating means transmits the first additional information, and

the second generating means receives the first additional information and sets the received first additional information as the second additional information.

4. The cryptocommunication system of Claim 1,

wherein the first generating means encrypts the first additional information according to the encryption algorithm to generate encrypted additional information, and transmits the generated encrypted additional information, and

the second generating means receives the encrypted additional information, and decrypts the received encrypted additional information according to the decryption algorithm which is an inverse-conversion of the encryption algorithm to generate additional information, and sets the generated additional information as the second additional information.

5. The cryptocommunication system of Claim 1,

wherein the first generating means generates a random number, and sets the generated random number as the first additional information.

6. The cryptocommunication system of Claim 1,

wherein the invertible operation means bit-connects the plaintext with the first additional information so as to generate the connected information, and

the second operation means deletes the second additional information from the decrypted connected information to generate the decrypted text.

7. The cryptocommunication system of Claim 1,

wherein the first operation means performs an exclusive OR operation on the plaintext and the first additional information to generate the connected information, and

the second operation means performs an exclusive OR operation on the decrypted connected information and the second additional information to generate the decrypted text.

8. The cryptocommunication system of Claim 1,

wherein the first operation means adds the first additional information to the plaintext to generate connected information, and

the second operation means subtracts the second additional information from the decrypted connected information to generate the decrypted text.

9. The cryptocommunication system of Claim 1,

wherein the first operation means performs modular multiplication on the plaintext and the first additional information to generate the connected information, and

the second operation means performs modular multiplication on the decrypted connected information and the modular inversion of the second additional information to generate the decrypted text.

10. The cryptocommunication system of Claim 1,

wherein the first operation means replaces the plaintext expressed in bit based on the first additional information to generate the connected information,

and the second operation means inverse-replaces the decrypted connected information expressed in bit based on the second additional information to generate the decrypted text.

11. The cryptocommunication system of Claim 1,

wherein the first operation means stores, in advance, a conversion table corresponding to the first additional information, and converts the plaintext according to the conversion table to generate the connected information, and

the second operation means stores, in advance, a conversion table corresponding to the second additional information and being identical to the conversion table corresponding to the first additional information, and converts the decrypted connected information in a reverse direction according to the conversion table to generate the decrypted text.

12. The cryptocommunication system of Claim 1,

wherein when the transmission apparatus encrypts, in order to generate ciphertext, the plaintext that has been encrypted and transmitted, and transmits the newly generated ciphertext to the reception apparatus,

and the reception apparatus receives the newly generated ciphertext and decrypts the newly generated ciphertext,

the first generating means generates third additional information which is different from the first additional information,

the first operation means performs an invertible operation on the plaintext and the third additional information to obtain newly generated connected information,

the encrypting means encrypts the newly generated connected information according to an encryption algorithm to obtain the newly generated ciphertext,

the transmitting means transmits the newly generated ciphertext,

the receiving means receives the newly generated ciphertext,

the second generating means generates forth additional information which is identical to the third additional information,

the decrypting means decrypts the newly generated ciphertext according to a decryption algorithm which is an inverse-conversion of the encryption algorithm to obtain newly generated decrypted connected information,

and the second operation means performs an inverse operation of the invertible operation on the newly generated decrypted connected information and the fourth additional information to obtain newly generated decrypted text.

13. The cryptocommunication system of Claim 1,

wherein the transmission apparatus performs the one-way function on the connected information instead of on the plaintext, in order to generate the first functional value,

the reception apparatus performs the one-way function on the decrypted connected information instead of on the decrypted text, in order to generate the second functional value,

and the reception apparatus judges whether the first and the second functional values match.

14. The cryptocommunication system of Claim 1,

wherein the transmission apparatus further performs, on the plaintext, a different invertible operation from the invertible operation, to generate first connected information,

the transmission apparatus performs the one-way function on the first connected information, instead of on the plaintext, to generate the first functional value,

the reception apparatus further performs the different invertible operation on the decrypted text to generate second connected information,

the reception apparatus performs the one-way function on the second connected information instead of on the decrypted text, to generate the second functional value,

and the reception apparatus judges whether the first and the second functional values match.

15. A cryptocommunication method used by a cryptocommunication system including a transmission apparatus and a reception apparatus,

the transmission apparatus encrypting plaintext to generate ciphertext, performing a one-way operation on the plaintext to generate a first value, and transmitting the ciphertext and the first value to the reception apparatus,

the reception apparatus receiving the ciphertext and the first value, decrypting the ciphertext to generate decrypted text, performing the one-way operation on the decrypted text to generate a second value, and judging that the decrypted text matches the plaintext when the second value and the first value match,

the cryptocommunication method including a transmission step which is executed by the transmission apparatus and a reception step which is executed by the reception apparatus,

the transmission step comprising:

a first generating substep for generating first additional information;

a first operation substep for performing an invertible operation on the plaintext and the first additional information to generate connected information;

an encrypting substep for encrypting the connected information according to an encryption algorithm to generate the ciphertext; and

a transmitting substep for transmitting the ciphertext,

the reception step comprising:

a receiving substep for receiving the ciphertext;

a second generating substep for generating second additional information which is identical to the first additional information;

a decrypting substep for decrypting the ciphertext according to a decryption algorithm which is an inverse-conversion of the encryption algorithm so as to generate decrypted connected information; and

a second operation substep for performing an inverse operation of the invertible operation on the decrypted connected information and the second additional information so as to generate the decrypted text.

16. Cryptocommunication program used by a cryptocommunication system including a transmission apparatus and a reception apparatus,

the transmission apparatus encrypting plaintext to generate ciphertext, performing a one-way operation on the plaintext to generate a first value, and transmitting the ciphertext and the first value to the reception apparatus,

the reception apparatus receiving the ciphertext and the first value, decrypting the ciphertext to generate decrypted text, performing the one-way operation on the decrypted text to generate a second value, and judging that the decrypted text matches the plaintext when the second value and the first value match,

the cryptocommunication program including a transmission step which is executed by the transmission apparatus and a reception step which is executed by the reception apparatus,

the transmission step comprising:

a first generating substep for generating first additional information;

a first operation substep for performing an invertible operation on the plaintext and the first additional information to generate connected information;

an encrypting substep for encrypting the connected information according to an encryption algorithm to generate the ciphertext; and

a transmitting substep for transmitting the ciphertext,

the reception step comprising:

a receiving substep for receiving the ciphertext;

second generating means for generating second additional information which is identical to the first additional information;

a decrypting substep for decrypting the ciphertext according to a decryption algorithm which is an inverse-conversion of the encryption algorithm so as to generate decrypted connected information; and

a second operation substep for performing an inverse operation of the invertible operation on the decrypted connected information and the second additional information so as to generate the decrypted text.

17. A recording medium which can be read from using a computer and which stores cryptocommunication program used by a cryptocommunication system including a transmission apparatus and a reception apparatus,

the transmission apparatus encrypting plaintext to generate ciphertext, performing a one-way operation on the plaintext to generate a first value, and transmitting the ciphertext and the first value to the reception apparatus,

the reception apparatus receiving the ciphertext and the first value, decrypting the ciphertext to generate decrypted text, performing the one-way operation on the decrypted text to generate a second value, and judging that the decrypted text matches the plaintext when the second value and the first value match,

the cryptocommunication program including a transmission step which is executed by the transmission apparatus and a reception step which is executed by the reception apparatus,

the transmission step comprising:

a first generating substep for generating first additional information;

a first operation substep for performing an invertible operation on the plaintext and the first additional information to generate connected information;

an encrypting substep for encrypting the connected information according to an encryption algorithm to generate the ciphertext; and

a transmitting substep for transmitting the ciphertext,

the reception step comprising:

a receiving substep for receiving the ciphertext;

a second generating substep for generating second additional information which is identical to the first additional information;

a decrypting substep for decrypting the ciphertext according to a decryption algorithm which is an inverse-conversion of the encryption algorithm so as to generate decrypted connected information; and a second operation substep for performing an inverse operation of the invertible operation on the decrypted connected information and the second additional information so as to generate the decrypted text.

18. A transmission apparatus which encrypts plaintext to generate ciphertext, performs a one-way operation on the plaintext to generate a first value, and transmits the ciphertext and the first value, the transmission apparatus comprising:

first generating means for generating first additional information;

first operation means for performing an invertible operation on the plaintext and the first additional information to generate connected information;

encrypting means for encrypting the connected information according to the encryption algorithm to generate ciphertext; and

transmitting means for transmitting the ciphertext.

19. A reception apparatus which receives, from a transmission apparatus, ciphertext and a first value, decrypts the ciphertext to generate decrypted text, performs the one-way operation on the decrypted text to generate a second value, and judges that the decrypted text corresponds to the

plaintext only when the second value and the first value match,

the transmission apparatus encrypting the plaintext to generate the ciphertext, performing the one-way operation on the plaintext to generate the first value, and transmitting the ciphertext and the first value,

the reception apparatus comprising:

receiving means for receiving the ciphertext from the transmission apparatus of Claim 18;

second generating means for generating second additional information which is identical to the first additional information;

decrypting means for decrypting the ciphertext according to a decryption algorithm which is an inverse-conversion of the encryption algorithm to generate decrypted connected information; and

second operation means for performing an inverse operation of the invertible operation on the decrypted connected information and the second additional information to generate decrypted text.